

POLYNOMIAL DEGREE BOUNDS FOR MATRIX SEMI-INVARIANTS

HARM DERKSEN AND VISU MAKAM

ABSTRACT. We study the left-right action of $\mathrm{SL}_n \times \mathrm{SL}_n$ on m -tuples of $n \times n$ matrices with entries in an infinite field K . We show that invariants of degree $n^2 - n$ define the null cone. Consequently, invariants of degree $\leq n^6$ generate the ring of invariants if $\mathrm{char}(K) = 0$. We also prove that for $m \gg 0$, invariants of degree at least $n\lfloor\sqrt{n+1}\rfloor$ are required to define the null cone. We generalize our results to matrix invariants of m -tuples of $p \times q$ matrices, and to rings of semi-invariants for quivers. For the proofs, we use new techniques such as the regularity lemma by Ivanyos, Qiao and Subrahmanyam, and the concavity property of the tensor blow-ups of matrix spaces. We will discuss several applications to algebraic complexity theory, such as a deterministic polynomial time algorithm for non-commutative rational identity testing, and the existence of small division-free formulas for non-commutative polynomials.

1. INTRODUCTION

1.1. Degree bounds for invariant rings. Let $\mathrm{Mat}_{p,q}$ be the set of $p \times q$ matrices with entries in an infinite field K . The group GL_n acts on $\mathrm{Mat}_{n,n}^m$ by simultaneous conjugation. Procesi showed that in characteristic 0, the invariant ring is generated by traces of words in the matrices. Razmyslov ([35, final remark]) showed that the invariant ring is generated by polynomials of degree $\leq n^2$ by studying trace identities (see also [13]). In positive characteristic, generators of the invariant ring were given by Donkin in [14, 15]. Domokos proved an upper bound $O(n^7 m^n)$ for the degree of generators (see [10, 11]).

In this paper we will focus on the left-right action of $G = \mathrm{SL}_n \times \mathrm{SL}_n$ on the space $V = \mathrm{Mat}_{n,n}^m$ of m -tuples of $n \times n$ matrices. This action is given by

$$(A, B) \cdot (X_1, X_2, \dots, X_m) = (AX_1B^{-1}, AX_2B^{-1}, \dots, AX_mB^{-1}).$$

The group G also acts on the graded ring $K[V]$ of polynomial functions on V , and the subring of G -invariant polynomials is denoted by $R(n, m) = K[V]^G$. This subring inherits a grading $R(n, m) = \bigoplus_{d=0}^{\infty} R(n, m)_d$. We have $R(n, m)_d = 0$ unless d is divisible by n (see Theorem 1.4). It is well-known that $R(n, 1)$ is generated by the determinant $\det(X_1)$, and $R(n, 2)$ is generated by the coefficients of $\det(X_1 + tX_2)$ as a polynomial in t . Because the group G is reductive, this invariant ring is finitely generated (see [20, 21, 30, 19]).

Definition 1.1. The number $\beta(n, m)$ is the smallest nonnegative integer d such that $R(n, m)$ is generated by invariants of degree $\leq d$.

The following bounds are known if K has characteristic 0:

- (1) $\beta(n, 1) = \beta(n, 2) = n$;
- (2) $\beta(1, m) = 1$;

The first author was supported by NSF grant DMS-1302032 and the second author was supported by NSF grant DMS-1361789.

- (3) $\beta(2, m) \leq 4$;
- (4) $\beta(3, 3) = 9$;
- (5) $\beta(3, m) \leq 309$;
- (6) $\beta(n, m) \geq n^2$ if $m \geq n^2$;
- (7) $\beta(n, m) = O(n^4((n+1)!)^2)$.

The bounds in (1) follow from the descriptions of $R(n, 1)$ and $R(n, 2)$ above and (2) is trivial. The bound (3) can be found in [8] (see also [25]). This bound also follows from the First Fundamental Theorem of Invariant Theory for SO_4 , because $\mathrm{SL}_2 \times \mathrm{SL}_2$ is a finite central extension of SO_4 and the representation $\mathrm{Mat}_{2,2}$ of $\mathrm{SL}_2 \times \mathrm{SL}_2$ corresponds to the standard 4-dimensional representation of SO_4 . The bound (4) was given in [9]. (5) and (6) were proved by the second author in [29]. Some explicit upper bounds for $\beta(3, m)$ for $m = 4, 5, 6, 7, 8$ that are sharper than (5) were also given in [29]. For the ring of invariants of a rational representation of a reductive group, there is a general bound on the degree of generating invariants (see [4] and [5, Section 4.7]). This bound gives $O(n^8 16^{n^2})$ and Ivanyos, Qiao and Subrahmanyam showed in [24, 25] that this bound can be improved to (7). We will improve this factorial bound to a polynomial one:

Theorem 1.2. *If K has characteristic 0, then we have $\beta(n, m) \leq mn^4$.*

A theorem of Weyl (see [27, Section 7.1, Theorem A]) essentially tells us that a bound on the degree of generating invariants for $R(n, n^2)$ will be a bound on the degree of generating invariants for $R(n, m)$ for all m . So we have:

Corollary 1.3. *If K has characteristic 0, then we have $\beta(n, m) \leq n^6$.*

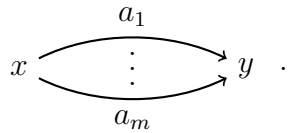
Given two matrices $A = (a_{ij})$ of size $m \times n$, and $B = (b_{ij})$ of size $p \times q$, we define their tensor (or Kronecker) product to be

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{m1}B & \cdots & \cdots & a_{mn}B \end{bmatrix} \in \mathrm{Mat}_{mp, nq}.$$

For $T = (T_1, T_2, \dots, T_m) \in \mathrm{Mat}_{d,d}^m$, we define an invariant $f_T \in R(n, m)$ of degree dn by

$$f_T(X_1, X_2, \dots, X_m) = \det(X_1 \otimes T_1 + X_2 \otimes T_2 + \cdots + X_m \otimes T_m).$$

Consider the generalized Kronecker quiver $\theta(m)$ which is a graph with 2 vertices x and y and m arrows from x to y .



Then $R(n, m)$ is the ring of semi-invariants for the quiver $\theta(m)$ and dimension vector (n, n) . Generators of $R(n, m)$ can be given in terms of determinants of certain block matrices, see [6, Corollary 3], [12] and [36]. These results, applied to the Kronecker quiver $\theta(m)$ give:

Theorem 1.4. *The invariant ring $R(n, m)$ is generated by all f_T with $T \in \mathrm{Mat}_{d,d}^m$ and $d \geq 1$.*

1.2. Hilbert's null cone. Hilbert's null cone $\mathcal{N} = \mathcal{N}(n, m) \subseteq V$ is the zero set of all non-constant homogeneous invariants in $R(n, m)$. The null cone plays an important role in Geometric Invariant Theory.

Definition 1.5. We define the constant $\gamma(n, m)$ as the smallest positive integer d such that the non-constant homogeneous invariants of degree $\leq d$ define the null cone.

If K has characteristic 0, then polynomial bounds for $\gamma(n, m)$ imply polynomial bounds for $\beta(n, m)$ (see [4]). From the description of the invariants in Theorem 1.4 follows:

Corollary 1.6. *The following statements are equivalent:*

- (1) $X = (X_1, X_2, \dots, X_m)$ does not lie in the null cone $\mathcal{N}(n, m)$;
- (2) $f_T(X) \neq 0$ for some $T \in \text{Mat}_{d,d}^m$ with $d \geq 1$.

Definition 1.7. Let $\delta(n, m)$ be the smallest positive integer k such that $X \notin \mathcal{N}(n, m)$ implies that there exists an integer d with $1 \leq d \leq k$ and an m -tuple $T = (T_1, \dots, T_m) \in \text{Mat}_{d,d}^m$ of $d \times d$ matrices, such that $f_T(X) \neq 0$. Since the f_T 's generate the invariant ring by Theorem 1.4, it is clear that $\gamma(n, m) = n\delta(n, m)$.

Theorem 1.8. *If $n \geq 2$, $X = (X_1, \dots, X_m) \notin \mathcal{N}(n, m)$ and $d \geq n-1$, then there exists an m -tuple $T \in \text{Mat}_{d,d}^m$ such that $f_T(X) \neq 0$. In particular $\delta(n, m) \leq n-1$ and $\gamma(n, m) \leq n(n-1)$.*

Lemma 1.9. *The function $\delta(n, m)$ is a weakly increasing function of m , and for $m > n^2$ we have $\delta(n, m) = \delta(n, n^2)$.*

Let us define $\delta(n) = \max_m \delta(n, m) = \delta(n, n^2)$ and $\gamma(n) = \gamma(n, n^2) = n\delta(n)$. We prove a lower bound on $\delta(n)$ which indicates that the upper bound we find in Theorem 1.8 is quite strong.

Theorem 1.10. *We have $\delta(n) \geq \lfloor \sqrt{n+1} \rfloor$ and $\gamma(n) \geq n \lfloor \sqrt{n+1} \rfloor$.*

1.3. Degree bounds for rings of quiver semi-invariants. For details and notational conventions we refer to Section 5. To a quiver Q with vertex set Q_0 , and a dimension vector $\alpha \in \mathbb{Z}_{\geq 0}^{Q_0}$ one can associate a ring $\text{SI}(Q, \alpha)$ of semi-invariants. This ring is graded by weights $\sigma \in \mathbb{Z}^{Q_0}$, so we have a decomposition $\text{SI}(Q, \alpha) = \bigoplus_{\sigma \in \mathbb{Z}_{\geq 0}^{Q_0}} \text{SI}(Q, \alpha)_{\sigma}$. For a given weight σ , we can consider the subring $\text{SI}(Q, \alpha, \sigma) = \bigoplus_{d=0}^{\infty} \text{SI}(Q, \alpha)_{d\sigma}$. For any weight σ , the projective variety $\text{Proj}(\text{SI}(Q, \alpha, \sigma))$, if nonempty, is a moduli space for the α -dimensional representations of the quiver Q . See [26] for more details.

In Section 5 we will give polynomial bounds (in terms of α, σ, Q) for the generators of $\text{SI}(Q, \alpha, \sigma)$. For the generalized Kronecker quiver $\theta(m)$ and dimension vector (p, q) this gives:

Theorem 1.11. *If $\text{char}(K) = 0$, then the invariant ring $K[\text{Mat}_{p,q}^m]^{\text{SL}_p \times \text{SL}_q}$ is generated by invariants of degree $\leq (pq \text{ lcm}(p, q))^2$.*

1.4. Applications to Algebraic Complexity Theory. The polynomial degree bound has some interesting applications in Algebraic Complexity Theory. Some applications are related to free skew fields. Suppose that $X = (X_1, X_2, \dots, X_m) \in \text{Mat}_{n,n}^m$ and consider the free skew field $L = K \langle t_1, t_2, \dots, t_m \rangle$ generated by t_1, t_2, \dots, t_m (see [3]). There is a useful criterion to test invertibility over the skew field (take $Q_0 = 0$ in [22, Proposition 7.3]):

Proposition 1.12. *The matrix $A = t_1X_1 + t_2X_2 + \cdots + t_mX_m \in \text{Mat}_{n,n}(L)$ is invertible, if and only if there exists a nonnegative integer d and matrices $T_1, T_2, \dots, T_m \in \text{Mat}_{d,d}(K)$ such that $X_1 \otimes T_1 + X_2 \otimes T_2 + \cdots + X_m \otimes T_m$ is invertible.*

Various problems in Algebraic Complexity Theory can be reduced to testing whether some linear matrix A is invertible. For this reason, Problem 4 in [22] asks for an upper bound for $\delta(n)$. The polynomial bound for $\delta(n)$ gives us a randomized polynomial time algorithm for determining whether the linear matrix $A = \sum_{i=1}^m t_iX_i \in \text{Mat}_{n,n}(L)$ is invertible for infinite fields of arbitrary characteristic. For $K = \mathbb{Q}$ it was shown by Garg, Gurvits, Oliveira and Wigderson in [17] that Gurvits' algorithm in [18] can decide invertibility of A in deterministic polynomial time polynomial over \mathbb{Q} , without using a polynomial bound on $\delta(n)$ (a weaker bound suffices). A similar result can be obtained by combining the results from [24] with our polynomial bound for $\delta(n)$. In Section 6 we will discuss in more detail, the following consequences from the polynomial bound.

- **Rational identity testing:** Deciding whether a non-commutative formula computes the zero function can be determined in randomized polynomial time, and in deterministic polynomial time when working over the field \mathbb{Q} .
- **Division-free formulas:** Given a non-commutative polynomial of degree k in m variables which has a formula of size n using additions, multiplications and divisions, then there exists a division-free formula of size $n^{O(\log^2(k)\log(n))}$.
- **Lower bounds on formula size:** Any formula with divisions computing the non-commutative determinant of degree n must have at least sub-exponential size (in n).

1.5. **Organisation.** In Section 2, we recall the language of linear subspaces and blow ups and prove Theorem 1.8. We prove the degree bounds for invariants defining the null cone and for generating invariants in Section 3. In Section 4, we explain a construction that allows to prove the lower bound in Theorem 1.10. In Section 5 we study degree bounds for quiver semi-invariants, and generalize the degree bound for matrix invariants to arbitrary rectangular matrices. In Section 6 we discuss applications to Algebraic Complexity Theory.

2. LINEAR SUBSPACES OF MATRICES AND BLOW UPS

Various properties of an m -tuple $X = (X_1, X_2, \dots, X_m) \in \text{Mat}_{n,n}^m$ only depend on the subspace spanned by X_1, \dots, X_m . In this section we study such subspaces.

Definition 2.1. Let \mathcal{X} be a linear subspace of $\text{Mat}_{k,n}$. We define $\text{rank}(\mathcal{X})$ to be the maximal rank among its members,

$$\text{rank}(\mathcal{X}) = \max\{\text{rank}(X) \mid X \in \mathcal{X}\}.$$

We define tensor blow ups of linear subspaces following [24].

Definition 2.2. Let \mathcal{X} be a linear subspace of $\text{Mat}_{k,n}$. We define its (p, q) tensor blow up $\mathcal{X}^{\{p,q\}}$ to be

$$\mathcal{X} \otimes \text{Mat}_{p,q} = \left\{ \sum_i X_i \otimes T_i \mid X_i \in \mathcal{X}, T_i \in \text{Mat}_{p,q} \right\}$$

viewed as a linear subspace of $\text{Mat}_{kp,nq}$. We will write $\mathcal{X}^{\{d\}} = \mathcal{X}^{\{d,d\}}$.

In [24], Ivanyos, Qiao and Subrahmanyam prove a regularity lemma ([24, Lemma 11 and Remark 10]) which is crucial for the proof of our main results.

Proposition 2.3 ([24]). *If \mathcal{X} is a linear subspace of matrices, then $\text{rank}(\mathcal{X}^{\{d\}})$ is a multiple of d .*

Let us fix $X = (X_1, \dots, X_m) \in \text{Mat}_{n,n}^m$ and let \mathcal{X} be the span of X_1, \dots, X_m . The following lemma is clear.

Lemma 2.4. *Given a positive integer d , the following statements are equivalent:*

- (1) *there exists an m -tuple $T \in \text{Mat}_{d,d}^m$ such that $f_T(X) \neq 0$;*
- (2) $\text{rank}(\mathcal{X}^{\{d\}}) = dn$.

Proof of Lemma 1.9. Let $X = (X_1, \dots, X_m) \in \text{Mat}_{n,n}^m$ and define $\overline{X} = (X_1, \dots, X_m, 0) \in \text{Mat}_{n,n}^{m+1}$. We have

$$X \notin \mathcal{N}(n, m) \Leftrightarrow \text{there exists a } d > 0 \text{ such that } \text{rank}(\mathcal{X}^{\{d\}}) = dn \Leftrightarrow \overline{X} \notin \mathcal{N}(n, m+1).$$

Suppose that $X \notin \mathcal{N}(n, m)$. Then we have $\overline{X} \notin \mathcal{N}(n, m+1)$. So there exists $T \in \text{Mat}_{d,d}^{m+1}$ with $f_T(\overline{X}) \neq 0$ and $d \leq \delta(n, m+1)$. It follows that $\text{rank}(\mathcal{X}^{\{d\}}) = dn$ so there exists $T \in \text{Mat}_{d,d}^m$ with $f_T(X) \neq 0$. This proves $\delta(n, m) \leq \delta(n, m+1)$.

If $m > n^2$ and $X \in \text{Mat}_{n,n}^m \setminus \mathcal{N}(n, m)$, then \mathcal{X} can be spanned by n^2 matrices, say Y_1, \dots, Y_{n^2} . If $Y = (Y_1, \dots, Y_{n^2})$ then there exists $S \in \text{Mat}_{d,d}^{n^2}$ with $f_S(Y) \neq 0$ and $d \leq \delta(n, n^2)$. So we have $\text{rank}(\mathcal{X}^{\{d\}}) = dn$, and there exists $T \in \text{Mat}_{d,d}^m$ with $f_T(X) \neq 0$. This proves that $\delta(n, m) \leq \delta(n, n^2)$. \square

Definition 2.5. We define the function $r : \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ by

$$r(p, q) = \text{rank}(\mathcal{X}^{\{p,q\}}).$$

Remark 2.6. Note that the set of all $T = (T_1, \dots, T_m) \in \text{Mat}_{p,q}^m$ for which $\sum_{i=1}^m X_i \otimes T_i$ has maximal rank $r(p, q)$ is Zariski dense in $\text{Mat}_{p,q}^m$.

Lemma 2.7. *The function r has the following properties:*

- (1) $r(p, q+1) \geq r(p, q)$;
- (2) $r(p+1, q) \geq r(p, q)$;
- (3) $r(p, q+1) \geq \frac{1}{2}(r(p, q) + r(p, q+2))$;
- (4) $r(p+1, q) \geq \frac{1}{2}(r(p, q) + r(p+2, q))$;
- (5) $r(p, q)$ is divisible by $\gcd(p, q)$.

Proof.

(1) follows from viewing $\mathcal{X}^{\{p,q\}}$ as a subspace of $\mathcal{X}^{\{p,q+1\}}$.

Now we will prove (3). Let $T = (T_1, \dots, T_m) \in \text{Mat}_{p,q+2}^m$. For a subset $J \subseteq \{1, 2, \dots, q+2\}$, let T_i^J be the submatrix where all the columns with index in J are omitted, and let \mathcal{Y}_J be the column span of $\sum_i X_i \otimes T_i^J$. If we choose T general enough, then $\sum_i X_i \otimes T_i^J$ will have rank $r(p, q+2 - |J|)$ for all $J \subseteq \{1, 2, \dots, q+2\}$. We have $\mathcal{Y}_1 + \mathcal{Y}_2 = \mathcal{Y}_\emptyset$ and $\mathcal{Y}_{1,2} \subseteq \mathcal{Y}_1 \cap \mathcal{Y}_2$. It follows that

$$r(p, q) = \dim \mathcal{Y}_{1,2} \leq \dim \mathcal{Y}_1 \cap \mathcal{Y}_2 = \dim \mathcal{Y}_1 + \dim \mathcal{Y}_2 - \dim(\mathcal{Y}_1 + \mathcal{Y}_2) = 2r(p, q+1) - r(p, q+2).$$

Parts (2) and (4) follow from (1) and (3) respectively by symmetry.

To see (5), write $p = dp'$ and $q = dq'$. Then we have $\mathcal{X}^{\{p,q\}} = (\mathcal{X}^{\{p',q'\}})^{\{d\}}$ and the result follows from Proposition 2.3. \square

In the above lemma, parts (1) and (3) give us that $r(p, q)$ is weakly increasing and weakly concave in the second variable, and parts (2) and (4) give the same conclusion for the first variable.

Corollary 2.8. *The function $r(p, q)$ is weakly increasing and weakly concave in either variable.*

Lemma 2.9. *If $r(1, 1) = 1$, then we have $r(d, d) = d$ for all d .*

Proof. Choose a nonzero matrix $A \in \mathcal{X}$ of rank 1. Using left and right multiplication with matrices in $\text{GL}_n(K)$ we may assume without loss of generality that

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

It is clear that $r(d, d) \geq d$. If $i > 1$, $j > 1$ and $B \in \mathcal{X}$ then $B_{i,j}$ has to be zero, otherwise $tA + B$ will have rank at least 2 for some t . So \mathcal{X} is contained in

$$\begin{bmatrix} * & * & \cdots & * \\ * & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & 0 & \cdots & 0 \end{bmatrix}.$$

Because all matrices of \mathcal{X} have rank at most 1, \mathcal{B} must be contained in the union $W_1 \cup W_2$, where

$$W_1 = \begin{bmatrix} * & 0 & \cdots & 0 \\ * & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ * & 0 & \cdots & 0 \end{bmatrix} \quad \text{and} \quad W_2 = \begin{bmatrix} * & * & \cdots & * \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Because \mathcal{X} is a subspace, it is entirely contained in W_1 or in W_2 . Now it is clear that the matrices in $\mathcal{X}^{\{d\}}$ have at most d nonzero columns, or at most d nonzero rows, so $r(d, d) \leq d$. \square

Proposition 2.10. *Let $n \geq 2$, and let $d + 1 \geq n$. If $r(d + 1, d + 1) = n(d + 1)$, then $r(d, d) = nd$ as well.*

Proof. Suppose that $r(d + 1, d + 1) = n(d + 1)$. If $1 \leq a \leq d$, then weak concavity implies that

$$r(d + 1, a) \geq \frac{(d + 1 - a)r(d + 1, 0) + ar(d + 1, d + 1)}{d + 1} = \frac{an(d + 1)}{d + 1} = an.$$

The inequality $r(d + 1, a) \leq an$ is clear, so $r(d + 1, a) = an$. Similarly, we have $r(a, d + 1) = an$. If $r(1, 1) = 1$ then we get $r(d + 1, d + 1) = d + 1$ by Lemma 2.9 which contradicts $r(d + 1, d + 1) = n(d + 1)$. So we have $r(1, 1) \geq 2$. Since $r(p, q)$ is weakly concave in the second variable, we have

$$r(1, d) \geq \frac{(d - 1) \cdot r(1, d + 1) + 1 \cdot r(1, 1)}{d} \geq \frac{(d - 1)n + 2}{d} = n - \frac{n - 2}{d} > n - 1,$$

where the last inequality follows as $d \geq n - 1$. Since $r(1, d)$ must be an integer, we have $r(1, d) \geq n$. Now, by the weak concavity in the first variable, we have

$$r(d, d) \geq \frac{(d-1) \cdot r(d+1, d) + 1 \cdot r(1, d)}{d} \geq \frac{(d-1)nd + n}{d} = nd - n + \frac{n}{d}.$$

Note that since $d \geq n - 1$, we have $d + \frac{n}{d} > n$ or equivalently that $-n + \frac{n}{d} > -d$. Thus, we have

$$r(d, d) \geq nd - n + \frac{n}{d} > d(n-1).$$

Recall that $r(d, d)$ must be a multiple of d by Lemma 2.3. Thus $r(d, d) = nd$. □

Proof of Theorem 1.8. Suppose $(X_1, X_2, \dots, X_m) \notin \mathcal{N}(n, m)$. By Lemma 2.4, $r(d, d) = dn$ for some d . Without loss of generality, we can assume $d \geq n$. By repeated application of Proposition 2.10, we conclude that $r(n-1, n-1) = n(n-1)$. So, again by Lemma 2.4, there exists an m -tuple $T = (T_1, \dots, T_m) \in \text{Mat}_{n-1, n-1}^m$ such that $f_T(X) \neq 0$. □

3. DEGREE BOUNDS ON GENERATING INVARIANTS

Suppose that the base field K has characteristic 0, G is a connected semisimple group and V is a representation of G . A homogeneous system of parameters for the invariant ring $K[V]^G$ is a set of homogeneous invariants f_1, f_2, \dots, f_r such that f_1, f_2, \dots, f_r are algebraically independent and $K[V]^G$ is a finitely generated $K[f_1, \dots, f_r]$ -module. The ring $K[V]^G$ is a finitely generated $K[f_1, \dots, f_r]$ -module if and only if the zero set of f_1, \dots, f_r is the null cone (see[21]).

Definition 3.1. For a representation V of a connected semisimple group G , $\beta(K[V]^G)$ is defined as the smallest integer d such that invariants of degree $\leq d$ generate the ring of invariants $K[V]^G$.

Using the homogeneous system of parameters in Corollary 3.3, we can get a bound for the generating invariants (see [32, 33] and [5, Corollary 2.6.3]):

Proposition 3.2. Suppose V is a representation of a connected semisimple group G . Let f_1, f_2, \dots, f_r be a homogeneous system of parameters for $K[V]^G$, and let $d_i = \deg(f_i)$. Then

$$\beta(K[V]^G) \leq \max\{d_1 + d_2 + \dots + d_r - r, d_1, d_2, \dots, d_r\}.$$

We go back to the special case where $V = \text{Mat}_{n,n}^m$, $G = \text{SL}_n \times \text{SL}_n$, and $\beta(n, m) = \beta(K[V]^G)$.

Corollary 3.3. Let $n \geq 2$, and let r be the Krull dimension of $R(n, m)$. Then there exist r invariants of degree $n^2 - n$ that form a homogeneous system of parameters.

Proof. By Theorem 1.8, the invariants of degree $n^2 - n$ define the null cone. We apply the Noether normalization lemma (see [5, Lemma 2.4.7]) to conclude that there exists r invariants of degree $n^2 - n$ that form a homogeneous system of parameters. □

Proof of Theorem 1.2. For $n \geq 2$, we apply the above proposition to the left-right action of $\text{SL}_n \times \text{SL}_n$ on n^2 -tuples of matrices using the homogeneous system of parameters from Corollary 3.3 to get

$$\beta(n, m) \leq r(n^2 - n) - r = r(n^2 - n - 1) \leq mn^2(n^2 - n - 1) < mn^4.$$

It is clear that $\beta(R(1, m)) = 1$, so we have $\beta(R(n, m)) \leq mn^4$ for all n and m . \square

4. LOWER BOUNDS FOR $\gamma(n)$ AND $\delta(n)$

In this section we prove Theorem 1.10. Let $A = t_1X_1 + t_2X_2 + \cdots + t_mX_m$ be an $n \times n$ linear matrix. The $(i, j)^{th}$ entry of A is a linear function in the indeterminates t_k 's with coefficients in K . In fact if $c_k \in K$ is the $(i, j)^{th}$ entry of X_k , then the $(i, j)^{th}$ entry of A is given by

$$A_{i,j} = \sum_{k=1}^m c_k t_k.$$

For $p \times p$ matrices T_1, T_2, \dots, T_m , observe that the expression $\sum_{k=1}^m X_k \otimes T_k$ is an $n \times n$ block matrix and the size of each block is $p \times p$. Moreover, the $(i, j)^{th}$ block is

$$\sum_{k=1}^m c_k T_k.$$

Remark 4.1. In effect $\sum_{k=1}^m X_k \otimes T_k$ is simply the block matrix obtained by substituting the T_k for t_k in the linear matrix A .

Lemma 4.2. *If there exist $k \times k$ matrices T_1, T_2, \dots, T_k such that $X_1 \otimes T_1 + \cdots + X_k \otimes T_k$ is invertible, then there exists $k \times k$ matrices S_2, S_3, \dots, S_k such that $X_1 \otimes I + X_2 \otimes S_2 + \cdots + X_k \otimes S_k$ is invertible.*

Proof. If there are exists T_1, T_2, \dots, T_k such that $\sum_{i=1}^m X_i \otimes T_i$ is invertible, then this matrix will be invertible for general choices of T_1, \dots, T_k . In particular, without loss of generality we may assume that T_1 invertible. If we set $S_i = T_1^{-1}T_i$ for $i \geq 2$, then we have

$$(I \otimes T_1)^{-1} \sum_{i=1}^m X_i \otimes T_i = X_1 \otimes I + X_2 \otimes S_2 + \cdots + X_k \otimes S_k$$

is invertible. \square

Given the remark and lemma above, we now state a straightforward lemma which follows from the definition of $\delta(n)$.

Lemma 4.3. *Suppose we have $X = (X_1, \dots, X_m) \in \text{Mat}_{n,n}^m$ and suppose that the linear matrix $A = \sum_{i=1}^m t_i X_i$ has the properties:*

- (1) *For any $k < d$, substituting $t_1 = I$ and substituting any $k \times k$ matrices for the indeterminates t_2, t_3, \dots, t_m gives us a singular matrix;*
- (2) *there exists a particular substitution of $d \times d$ matrices for t_1, t_2, \dots, t_m which gives a non-singular matrix.*

Then we have $\delta(n, m) \geq d$ and $\delta(n) \geq d$.

One can use the procedure in [22, Section 6] to construct a linear matrix in which the top right corner entry of its inverse (over the skew field) is any desired rational expression. For any d , we can find non-trivial rational expressions which are not defined for matrices of size $< d$, such as taking the inverse of the famous Amitsur-Levitzki polynomial (see [1]). However, the size of the linear matrix becomes very large giving us very weak bounds.

To find better bounds, we want to keep the size of n as small as possible, and we present the most efficient that we are able to find. We make use of the Cayley-Hamilton theorem,

which says that a matrix satisfies its characteristic polynomial. For the sake of clarity, we discuss it in detail for $d = 3$, and then describe the general construction.

For this construction, A, B , and C will denote arbitrary $k \times k$ matrices, and I will denote the identity matrix of size $k \times k$. First consider the block matrix

$$N_3 = \begin{bmatrix} A^2B & AB & B \\ A^2C & AC & C \\ A^2 & A & I \end{bmatrix}.$$

If $k \leq 2$, then the characteristic polynomial of A gives us a linear dependency in the columns. For example, if $k = 2$ and the characteristic polynomial of A is $t^2 + at + b$, then we have

$$\begin{bmatrix} A^2B & AB & B \\ A^2C & AC & C \\ A^2 & A & I \end{bmatrix} \begin{bmatrix} I \\ aI \\ bI \end{bmatrix} = 0.$$

However, if we pick

$$(1) \quad A = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \text{ and } C = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},$$

with the λ_i pairwise distinct, then

$$N_3 = \left[\begin{array}{ccc|ccc|ccc} 0 & 0 & \lambda_1^2 & 0 & 0 & \lambda_1 & 0 & 0 & 1 \\ \lambda_2^2 & 0 & 0 & \lambda_2 & 0 & 0 & 1 & 0 & 0 \\ 0 & \lambda_3^2 & 0 & 0 & \lambda_3 & 0 & 0 & 1 & 0 \\ \hline 0 & \lambda_1^2 & 0 & 0 & \lambda_1 & 0 & 0 & 0 & 1 \\ 0 & 0 & \lambda_2^2 & 0 & 0 & \lambda_2 & 0 & 0 & 1 \\ \lambda_3^2 & 0 & 0 & \lambda_3 & 0 & 0 & 1 & 0 & 0 \\ \hline \lambda_1^2 & 0 & 0 & \lambda_1 & 0 & 0 & 1 & 0 & 0 \\ 0 & \lambda_2^2 & 0 & 0 & \lambda_2 & 0 & 0 & 1 & 0 \\ 0 & 0 & \lambda_3^2 & 0 & 0 & \lambda_3 & 0 & 0 & 1 \end{array} \right].$$

Permuting the rows of N_3 , we get

$$\left[\begin{array}{ccc|ccc|ccc} \lambda_1^2 & 0 & 0 & \lambda_1 & 0 & 0 & 1 & 0 & 0 \\ \lambda_2^2 & 0 & 0 & \lambda_2 & 0 & 0 & 1 & 0 & 0 \\ \lambda_3^2 & 0 & 0 & \lambda_3 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & \lambda_1^2 & 0 & 0 & \lambda_1 & 0 & 0 & 1 & 0 \\ 0 & \lambda_2^2 & 0 & 0 & \lambda_2 & 0 & 0 & 1 & 0 \\ 0 & \lambda_3^2 & 0 & 0 & \lambda_3 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & \lambda_1^2 & 0 & 0 & \lambda_1 & 0 & 0 & 1 \\ 0 & 0 & \lambda_2^2 & 0 & 0 & \lambda_2 & 0 & 0 & 1 \\ 0 & 0 & \lambda_3^2 & 0 & 0 & \lambda_3 & 0 & 0 & 1 \end{array} \right].$$

Then permuting the columns, we get

$$\left[\begin{array}{ccc|ccc|ccc} \lambda_1^2 & \lambda_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_2^2 & \lambda_2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_3^2 & \lambda_3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & \lambda_1^2 & \lambda_1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_2^2 & \lambda_2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_3^2 & \lambda_3 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & \lambda_1^2 & \lambda_1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_2^2 & \lambda_2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_3^2 & \lambda_3 & 1 \end{array} \right],$$

and hence N_3 is non-singular as the λ_i are pairwise distinct. The one problem with using this directly is the non-linearity of the entries in N_3 . To fix this, we consider the 8×8 block matrix

$$F_3 = \left[\begin{array}{ccc|ccc|ccc} I & & & & & & B & & \\ -A & I & & & & & & B & \\ & & -A & & & & & & B \\ \hline & & & I & & & C & & \\ & & & -A & I & & & C & \\ & & & & & -A & & & C \\ \hline & & & & & & I & A & \\ & & & & & & -A & A & I \end{array} \right].$$

The invertibility of such a block matrix is unaffected by adding left multiplied block rows to other block rows, and by adding right multiplied block columns to other block columns. We left multiply the first block row by A and add it to the second block row. Then we left multiply the second block row by A and add it to the third block row. Focusing on the top three block rows, we have transformed

$$\left[\begin{array}{ccc|ccc} I & & & B & & \\ -A & I & & & B & \\ & & -A & & & B \end{array} \right] \longrightarrow \left[\begin{array}{ccc|ccc} I & & & B & & \\ & I & & AB & B & \\ & & -A & A^2B & AB & B \end{array} \right].$$

We can also right multiply block columns by a matrix and add them to other block columns. So, we can further transform the top 3 block rows to

$$\left[\begin{array}{ccc|ccc} I & & & A^2B & AB & B \\ & I & & & & \\ & & -A & & & \end{array} \right].$$

Notice that these transformations do not affect the rest of the block rows in F_3 . A similar procedure for the next 3 block rows, and then for the last two block rows shows that the

invertibility of F_3 is equivalent to the invertibility of

$$\left[\begin{array}{ccc|ccc} I & & & & & \\ & I & & & & \\ & & A^2B & AB & B & \\ \hline & & I & & & \\ & & & I & & \\ & & & & A^2C & AC & C \\ \hline & & & & I & & \\ & & & & & A^2 & A & I \end{array} \right],$$

which is then equivalent to the invertibility of N_3 .

Thus if A, B , and C are square matrices of size ≤ 2 , then F_3 is always singular. However, there exists a particular choice of 3×3 matrices, i.e, (1), for which F_3 is invertible. We can write F_3 as $X_1 \otimes I + X_2 \otimes A + X_3 \otimes B + X_4 \otimes C$ and consider $X = (X_1, X_2, X_3, X_4) \in \text{Mat}_{8,8}^4 \setminus \mathcal{N}(8, 4)$.

The above discussion shows that X satisfies the conditions of Lemma 4.3 for $n = 8, d = 3$, and so we get $\delta(8) \geq 3$.

For the general construction, consider

$$N_d = \begin{bmatrix} A^{d-1}B_1 & A^{d-2}B_1 & \cdots & B_1 \\ A^{d-1}B_2 & \ddots & & B_2 \\ \vdots & & \ddots & \vdots \\ A^{d-1}B_{d-1} & \cdots & \cdots & B_{d-1} \\ A^{d-1} & \cdots & \cdots & I \end{bmatrix},$$

where A, B_i are taken to be arbitrary $k \times k$ matrices. If $k < d$, then the characteristic polynomial of A gives a linear dependency on the columns. On the other hand, choose A to be a diagonal $d \times d$ matrix with pairwise distinct diagonal entries $\lambda_1, \lambda_2, \dots, \lambda_d$, choose B_1 to be the permutation matrix corresponding to the long cycle in the symmetric group on d letters, and choose $B_i = B_1^i$. Similar to the case of N_3 , we can permute the rows and columns to transform it into a block diagonal matrix, where each diagonal block is a Vandermonde matrix, and hence invertible.

Similiar to the construction of F_3 , we construct F_d and this has size $d^2 - 1 \times d^2 - 1$. To do this, we define an $n \times n - 1$ block matrix $\mathcal{P}_n(A)$ and an $n - 1 \times n$ block matrix $\mathcal{Q}_n(A)$ by

$$\mathcal{P}_n(A) = \begin{bmatrix} I & & & \\ -A & I & & \\ & \ddots & \ddots & \\ & & -A & I \\ & & & -A \end{bmatrix}, \text{ and } \mathcal{Q}_n(A) = \begin{bmatrix} A & 0 & & \\ & A & \ddots & \\ & & \ddots & 0 \\ & & & A & I \end{bmatrix}.$$

Notice that F_3 is just the block matrix

$$\begin{bmatrix} \mathcal{P}_3(A) & & I_3 \otimes B \\ & \mathcal{P}_3(A) & I_3 \otimes C \\ & & \mathcal{P}_2(A) & \mathcal{Q}_3(A) \end{bmatrix},$$

where I_3 denotes the identity matrix of size 3×3 . Now we define

$$F_d = \begin{bmatrix} \mathcal{P}_d(A) & & & & I_d \otimes B_1 \\ & \mathcal{P}_d(A) & & & I_d \otimes B_2 \\ & & \ddots & & \vdots \\ & & & \mathcal{P}_d(A) & I_d \otimes B_{d-1} \\ & & & \mathcal{P}_{d-1}(A) & \mathcal{Q}_d(A) \end{bmatrix},$$

where I_d denotes the identity matrix of size $d \times d$. We can write

$$F_d = X_1 \otimes I + X_2 \otimes A + X_3 \otimes B_1 + \cdots + X_{d+1} \otimes B_{d-1}$$

and we consider

$$X = (X_1, X_2, \dots, X_{d+1}) \in \text{Mat}_{d^2-1, d^2-1}^{d+1} \setminus \mathcal{N}(d^2-1, d+1).$$

A similar argument as in the case of $d = 3$, shows that the invertibility of F_d is equivalent to the invertibility of N_d . Thus, by Lemma 4.3, we have $\delta(d^2-1, d+1) \geq d$ and therefore $\delta(d^2-1) \geq d$. Replacing d^2-1 by n , we get $\delta(n) \geq \lfloor \sqrt{n+1} \rfloor$ and $\gamma(n) = n\delta(n) \geq n\lfloor \sqrt{n+1} \rfloor$.

5. GENERATING INVARIANTS FOR QUIVER REPRESENTATIONS

In this section, we generalize our degree bounds for matrix invariants to quiver representations. We start by introducing the common terminology. A quiver is just a directed graph. Formally a quiver is a pair $Q = (Q_0, Q_1)$, where Q_0 is a finite set of vertices and Q_1 is a finite set of arrows. For an arrow $a \in Q_1$ we denote its head and tail by ha and ta respectively. A path of length k is a sequence $p = a_k a_{k-1} \cdots a_1$ where a_1, \dots, a_k are arrows such that $ha_{i-1} = ta_i$ for $i = 2, 3, \dots, k$. The head and tail of the path are defined by $hp = ha_k$ and $tp = ta_1$ respectively. For every vertex $x \in Q_0$ we also have a trivial path ε_x of length 0 such that $h\varepsilon_x = t\varepsilon_x = x$. A cyclic path is a path p of positive length such that $hp = tp$. We will assume that Q has no cyclic paths.

We fix an infinite field K . A representation V of Q over K is a collection of finite dimensional K -vector spaces $V(x)$, $x \in Q_0$ together with a collection of K -linear maps $V(a) : V(ta) \rightarrow V(ha)$, $a \in Q_1$. The dimension vector of V is the function $\alpha : Q_0 \rightarrow \mathbb{Z}_{\geq 0}$ such that $\alpha(x) = \dim V(x)$ for all $x \in Q_0$. If $p = a_k a_{k-1} \cdots a_1$ is a path, then we define

$$V(p) = V(a_k)V(a_{k-1}) \cdots V(a_1) : V(tp) \rightarrow V(hp).$$

We define $V(\varepsilon_x)$ is the identity map from $V(x)$ to itself. For a dimension vector $\alpha \in \mathbb{Z}_{\geq 0}^{Q_0}$, we define its representation space by:

$$\text{Rep}(Q, \alpha) = \prod_{a \in Q_1} \text{Mat}_{\alpha(ha), \alpha(ta)}.$$

If V is a representation with dimension vector α and we identify $V(x) \cong K^{\alpha(x)}$ for all x , then V can be viewed as an element of $\text{Rep}(Q, \alpha)$. Consider the group $\text{GL}(\alpha) = \prod_{x \in Q_0} \text{GL}_{\alpha(x)}$ and its subgroup $\text{SL}(\alpha) = \prod_{x \in Q_0} \text{SL}_{\alpha(x)}$. The group $\text{GL}(\alpha)$ acts on $\text{Rep}(Q, \alpha)$ by:

$$(A(x) \mid x \in Q_0) \cdot (V(a) \mid a \in Q_1) = (A(ha)V(a)A(ta)^{-1} \mid a \in Q_1).$$

For $V \in \text{Rep}(Q, \alpha)$, choosing a different basis means acting by the group $\text{GL}(\alpha)$. The $\text{GL}(\alpha)$ -orbits in $\text{Rep}(Q, \alpha)$ correspond to isomorphism classes of representations of dimension α .

The group $\mathrm{GL}(\alpha)$ also acts (on the left) on the ring $K[\mathrm{Rep}(Q, \alpha)]$ of polynomial functions on $\mathrm{Rep}(Q, \alpha)$ by

$$A \cdot f(V) = f(A^{-1} \cdot V)$$

where $f \in K[\mathrm{Rep}(Q, \alpha)]$, $V \in \mathrm{Rep}(Q, \alpha)$ and $A \in \mathrm{GL}(\alpha)$.

The invariant ring $\mathrm{SI}(Q, \alpha) = K[\mathrm{Rep}(Q, \alpha)]^{\mathrm{SL}(\alpha)}$ is called the ring of semi-invariants. A multiplicative character of the group GL_α is of the form

$$\chi_\sigma : (A(x) \mid x \in Q_0) \in \mathrm{GL}_\alpha \mapsto \prod_{x \in Q_0} \det(A(x))^{\sigma(x)} \in K^\star,$$

where $\sigma : Q_0 \rightarrow \mathbb{Z}$ is called the weight of the character χ_σ . Define

$$\mathrm{SI}(Q, \alpha)_\sigma = \{f \in K[\mathrm{Rep}(Q, \alpha)] \mid \forall A \in \mathrm{GL}(\alpha) \ A \cdot f = \chi_\sigma(A)f\}.$$

Then we have $\mathrm{SI}(Q, \alpha) = \bigoplus_\sigma \mathrm{SI}(Q, \alpha)_\sigma$. If $\sigma \cdot \alpha = \sum_{x \in Q_0} \sigma(x)\alpha(x) \neq 0$, then $\mathrm{SI}(Q, \alpha)_\sigma = 0$. Assume that $\sigma \cdot \alpha = 0$. We can write $\sigma = \sigma_+ - \sigma_-$ where $\sigma_+(x) = \max\{\sigma(x), 0\}$ and $\sigma_-(x) = \max\{-\sigma(x), 0\}$. Define $n = \sigma_+ \cdot \alpha = \sigma_- \cdot \alpha$.

Now we define a linear matrix $n \times n$

$$A : \bigoplus_{x \in Q_0} V(x)^{\sigma_+(x)} \rightarrow \bigoplus_{x \in Q_0} V(x)^{\sigma_-(x)}$$

where each block $\mathrm{Hom}(V(x), V(y))$ is of the form $t_1 V(p_1) + \dots + t_r V(p_r)$ where t_1, t_2, \dots, t_r are indeterminates and p_1, p_2, \dots, p_r are all paths from x to y . We use different indeterminates for the different blocks, so the linear matrix has $m = \sum_{x \in Q_0} \sum_{y \in Q_0} \sigma_+(x) b_{x,y} \sigma_-(y)$ indeterminates where $b_{x,y}$ is the number of paths from x to y . We can write $A = t_1 X_1 + \dots + t_m X_m$ with $X_1, \dots, X_m \in \mathrm{Mat}_{n,n}$. We have the following result (see [6, Corollary 3], [12] and [36]).

Theorem 5.1. *The space $\mathrm{SI}(Q, \alpha)_\sigma$ is spanned by $\det(t_1 X_1 + \dots + t_m X_m)$ with $t_1, \dots, t_m \in K$.*

Corollary 5.2. *For any positive integer d , the space $\mathrm{SI}(Q, \alpha)_{d\sigma}$ is spanned by $\det(X_1 \otimes T_1 + \dots + X_m \otimes T_m)$ with $T_1, \dots, T_m \in \mathrm{Mat}_{d,d}$.*

Proof. This follows from the construction for $d\sigma$ instead of σ . □

Corollary 5.3. *We have a surjective ring homomorphism $\psi : K[\mathrm{Mat}_{n,n}^m]^{\mathrm{SL}_n \times \mathrm{SL}_n} \rightarrow \mathrm{SI}(Q, \alpha)$ which sends homogeneous elements of degree dn into $\mathrm{SI}(Q, \alpha)_{d\sigma}$.*

A representation $V \in \mathrm{Rep}(Q, \alpha)$ is called σ -semistable if there exists an semi-invariant $f \in \mathrm{SI}(Q, \alpha)_{d\sigma}$ with $f(V) \neq 0$ (see [26]).

Corollary 5.4. *If V is σ -semistable, $n = \sum_{x \in Q_0} \sigma_+(x)\alpha(x)$ and $d \geq n - 1$, then there exists an semi-invariant $f \in \mathrm{SI}(Q, \alpha)_{d\sigma}$ with $f(V) \neq 0$.*

The ring $\mathrm{SI}(Q, \alpha, \sigma) = \bigoplus_{d\sigma} \mathrm{SI}(Q, \alpha)_{d\sigma}$ is graded, where $\mathrm{SI}(Q, \alpha)_{d\sigma}$ is the degree d part.

Corollary 5.5. *The ring $\mathrm{SI}(Q, \alpha, \sigma)$ is generated in degree $\leq n^5$ where $n = \sum_{x \in Q_0} \sigma_+(x)\alpha(x)$.*

Let us consider again the Kronecker quiver $\theta(m)$, with dimension vector $\alpha = (p, q)$. Let $e = \gcd(p, q)$ and write $p = p'e$, $q = q'e$. Define $\sigma = (q', -p')$. We have $n = pq' = p'q = pq/e = pq/\gcd(p, q) = \mathrm{lcm}(p, q)$. We have $\mathrm{SI}(Q, \alpha) = \bigoplus_{d=0}^\infty \mathrm{SI}(Q, \alpha)_{d\sigma} = K[\mathrm{Mat}_{p,q}^m]^{\mathrm{SL}_p \times \mathrm{SL}_q}$. The null cone in this case is the set of representations that are not σ -semistable (see [26]). From Corollary 5.4 follows:

Corollary 5.6. *If $d \geq \text{lcm}(p, q) - 1$, then the null cone the action of $\text{SL}_p \times \text{SL}_q$ in $\text{Mat}_{p,q}^m$, is defined by invariants of degree $\leq \text{lcm}(p, q)d$.*

Proof of Theorem 1.11. Invariants of degree $\text{lcm}(p, q)^2$ define the null-cone. By the Noether normalization lemma, we can find a homogeneous system of parameters in degree $\text{lcm}(p, q)^2$. The number of elements in the homogeneous system of parameters is $\dim K[\text{Mat}_{p,q}^m]^{\text{SL}_p \times \text{SL}_q} \leq mpq$. So by Proposition 3.2, the ring $K[\text{Mat}_{p,q}^m]^{\text{SL}_p \times \text{SL}_q}$ is generated in degree $\leq mpq(\text{lcm}(p, q))^2$. Again by a theorem of Weyl (see [27, Section 7.1, Theorem A]), we may assume that $m \leq pq$. \square

6. APPLICATIONS TO ALGEBRAIC COMPLEXITY

We have already seen in the introduction that our results give a deterministic algorithm for the invertibility of a linear matrix over \mathbb{Q} . In [22], Hrubeš and Wigderson study non-commutative arithmetic circuits, and they comment that perhaps the most important problem that their work suggests is to find a good bound for $\delta(n)$. We describe the consequences of our bound for $\delta(n)$ in algebraic complexity.

A non-commutative arithmetic circuit is a directed acyclic graph, whose vertices are called gates. Gates of in-degree 0 are elements of K or variables t_i . The other allowed gates are inverse, addition and multiplication gates of in-degrees 1, 2 and 2 respectively. The edges going into an multiplication gate are labelled left and right to indicate the order of multiplication. A formula is a circuit, where every node has out-degree at most 1. The number of gates in a circuit is called its size. A non-commutative rational function over K in the variables t_1, t_2, \dots, t_m is an element of the skew field $L = K \langle t_1, t_2, \dots, t_m \rangle$. A circuit Φ in the variables t_1, t_2, \dots, t_m computes a non-commutative rational function for each output gate. We denote by $\hat{\Phi}(T)$ the evaluation of Φ at $T = (T_1, T_2, \dots, T_m) \in \text{Mat}_{p,p}^m$. In the process of evaluation, if the input of an inverse gate is not invertible, then $\hat{\Phi}(T)$ is undefined. Φ is called a correct circuit if $\hat{\Phi}(T)$ is defined for some T . For further details, we refer to [22].

Definition 6.1. The number $w(n)$ is the smallest integer d such that for every correct formula Φ of size n (in the variables t_1, t_2, \dots, t_m), there exists $T \in \text{Mat}_{p,p}^m$ with $p \leq d$ such that $\hat{\Phi}(T)$ is defined.

We have $w(n) \leq \delta(n^2 + n)$ by [22, Proposition 7.6]. However, due to the nature of our results, we can do even better.

Proposition 6.2. *We have $w(n) \leq 2n - 1$.*

Proof. Given a formula Φ of size n , for each gate v , we denote by Φ_v the sub-formula rooted at Φ . We can construct linear matrices A_{Φ_v} (in the variables t_1, t_2, \dots, t_m) such that Φ is a correct formula if and only if A_{Φ_v} is invertible (over the skew field L) for all v (see [22, Corollary 7.2]). Moreover the matrices A_{Φ_v} have size $\leq 2n$ (see [22, Theorem 2.5]).

Assume Φ is a correct formula. Since $A_{\Phi_v} = X_0 + t_1 X_1 + t_2 X_2 + \dots + t_m X_m$ is invertible, for some k there exists $T = (T_1, T_2, \dots, T_m) \in \text{Mat}_{k,k}^m$ such that $A_{\Phi_v}(T) = X_0 \otimes I + \sum_{i=1}^m X_i \otimes T_i$ is invertible (see Proposition 1.12 and Lemma 4.2). We can assume $k = 2n - 1$ by Proposition 2.10. In fact, by Remark 2.6 a general m -tuple $T \in \text{Mat}_{2n-1, 2n-1}^m$ suffices. Hence

for a sufficiently general $T \in \text{Mat}_{2n-1, 2n-1}^m$, all the $A_{\Phi_v}(T)$ are simultaneously invertible and hence $\widehat{\Phi}(T)$ is defined (see [22, Proposition 7.1]). \square

Rational identity testing. Deciding whether a non-commutative formula computes the zero function is called the rational identity testing problem. Hrubeš and Wigderson give a randomized algorithm for rational identity testing whose run time is polynomial in n and $w(n)$. See [22, Section 7] for the details. Thus the above bound on $w(n)$ gives a polynomial time randomized algorithm for rational identity testing for infinite fields in arbitrary characteristic.

As observed in [17], we have a deterministic polynomial time algorithm if $K = \mathbb{Q}$, since the invertibility of linear matrices can be decided in deterministic polynomial time.

Eliminating inverse gates. Let f be a non-commutative polynomial in $K\langle t_1, t_2, \dots, t_m \rangle$ of degree k , which can be computed by a formula of size n . Then f can be computed by a formula of size $n^{O(\log^2(k) \log(n))}$ without inverse gates. (see [22, Corollary 8.4]).

Lower bounds on formula size. Problem 1 in [22] asks for an explicit family of non-commutative polynomials which cannot be computed by a polynomial size formula with divisions. We give an answer to this problem. In [31], it was proved that any formula without divisions computing the non-commutative determinant (or permanent) of degree k must have size $2^{\Omega(k)}$. To find the size of a formula that allows divisions, we use our bound for eliminating inverse gates, and solve $2^{\Omega(k)} = n^{O(\log^2(k) \log(n))}$ for n . This shows that any formula with divisions computing the non-commutative determinant (or permanent) of degree k has size $2^{\Omega(\sqrt{k}/\log(k))}$.

Acknowledgements. The authors like to thank Avi Wigderson and Ketan Mulmuley for helpful discussions. We would like to thank the authors of [24, 22, 17, 28] for sending early versions of their papers.

REFERENCES

- [1] A. S. Amitsur and J. Levitzki, *Minimal identities for algebras*, Proceedings of the AMS **1** (1950), 449–463.
- [2] P. M. Cohn, *The embedding of firs in skew fields*, Proceedings of the London Math. Soc. **23** (1971), 193–213.
- [3] P. M. Cohn, *Skew Fields, Theory of General Division Rings*, Encyclopedia of Mathematics and its Applications **57**, Cambridge University Press, Cambridge, 1995.
- [4] H. Derksen, *Polynomial bounds for rings of invariants*, Proc. Amer. Math. Soc. **129** (2001), no. 4, 955–963.
- [5] H. Derksen and G. Kemper, *Computational Invariant Theory*. Invariant Theory and Algebraic Transformation Groups. I. Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, 2002.
- [6] H. Derksen and J. Weyman, *Semi-invariants of quivers and saturation of Littlewood-Richardson coefficients*, Journal of the American Math. Soc. **13** (2000), 467–479.
- [7] H. Derksen and J. Weyman, *On Littlewood-Richardson polynomials*, Journal of Algebra **255** (2002), 247–257.
- [8] M. Domokos, *Poincaré series of semi-invariants of 2×2 matrices*, Linear Algebra and its Applications **310** (2000), 183–194.
- [9] M. Domokos, *Relative invariants of 3×3 matrix triples*, Linear and Multilinear Algebra **47** (2000), 175–190.
- [10] M. Domokos, *Finite generating system of matrix invariants*, Math. Pannon **13** (2002), 175–181.

- [11] M. Domokos, S. G. Kuzmin and A. N. Zubkov, *Rings of matrix invariants in positive characteristic*, J. of Pure and Applied Algebra **176** (2002), 61–80.
- [12] M. Domokos and A. N. Zubkov, *Semi-invariants of quivers as determinants*, Transformation groups **6** (2001), 9–24.
- [13] E. Formanek, *Generating the ring of matrix invariants*, in: F. M. J. van Oystaeyen, editor, *Ring Theory*, Lecture Notes in mathematics **1197**, Springer Berlin Heidelberg, 1986, 73–82.
- [14] S. Donkin, *Invariants of several matrices*, Invent. Math. **110** (1992), 389–401.
- [15] S. Donkin, *Invariant functions on matrices*, Math. Proc. of the Cambridge Math. Soc. **113** (1993), 23–43.
- [16] M. Fortin and C. Reutenauer, *Commutative/non-commutative rank of linear matrices and subspaces of matrices of low rank*, Sémin. Lothar. Combin. 52:B52f, 2004.
- [17] A. Garg, L. Gurvits, R. Oliveira and A. Wigderson, *A deterministic polynomial time algorithm for non-commutative rational identity testing*, [arXiv:1511.03730](#), 2015.
- [18] L. Gurvits, *Classical complexity and quantum entanglement*, Journal of Computer and System Sciences **69** (2004), 448–484.
- [19] W. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. **102** (1975), 67–85.
- [20] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.
- [21] D. Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–370.
- [22] P. Hrubeš and A. Wigderson, *Non-commutative arithmetic circuits with division*, ITCS’14, Princeton, NJ, USA, 2014.
- [23] G. Ivanyos, M. Karpinski, Y. Qiao and M. Santha, *Generalized Wong sequences and their applications to Edmonds’ problems*, J. Comput. System Sci. **81** (2015), 1373–1386.
- [24] G. Ivanyos, Y. Qiao and K. V. Subrahmanyam, *Non-commutative Edmonds’ problem and matrix semi-invariants* [arXiv:1508.00690 \[cs.DS\]](#), 2015.
- [25] G. Ivanyos, Y. Qiao and K. V. Subrahmanyam, *On generating the ring of matrix semi-invariants*, [arXiv:1508.01554 \[cs.CC\]](#), 2015.
- [26] A. D. King, *Moduli of representations of finite-dimensional algebras*, Quart. J. Math. Oxford Ser. **45** (1994), no. 180, 515–530.
- [27] H. Kraft and C. Procesi, *Classical Invariant Theory : A primer*. <http://www.unibas.math.ch>.
- [28] K. Mulmuley, *Geometric Complexity Theory V: Equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether’s normalization lemma*, [arXiv:1209.5993](#).
- [29] V. Makam, *Hilbert series and degree bounds for matrix (semi-)invariants*, [arXiv:1510.08420 \[math.RT\]](#), 2015.
- [30] M. Nagata, *Invariants of a group in an affine ring*, J. Math. Kyoto Univ. **3** (1963/1964), 369–377.
- [31] N. Nisan, *Lower bounds for non-commutative computation*, In *Proceedings of the 23rd STOC* (1991), 410–418.
- [32] V. L. Popov, *Constructive Invariant Theory*, Astérisque **87–88** (1981), 303–334.
- [33] V. L. Popov, *The constructive theory of invariants*, Math. USSR Izvest. **10** (1982), 359–376.
- [34] C. Procesi, *The invariant theory of $n \times n$ matrices*, Adv. in Math. **19** (1976), 306–381.
- [35] Y. Razmyslov, *Trace identities of full matrix algebras over a field of characteristic zero*, Comm. in Alg. **8** (1980), Math. USSR Izv. **8** (1974), 727–760.
- [36] A. Schofield and M. van der Bergh, *Semi-invariants of quivers for arbitrary dimension vectors*, Indag. Mathem., N.S **12** (2001), 125–138.